STAT

Union Calendar No. 640

100TH CONGRESS *2d Session*	HOUSE OF REPRESENTATIVES	REPORT 100-1094

U.S. COUNTERINTELLIGENCE AND SECURITY CONCERNS: A STATUS REPORT

PERSONNEL AND INFORMATION SECURITY

REPORT

OF THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE
HOUSE OF REPRESENTATIVES

PREPARED BY THE

SUBCOMMITTEE ON OVERSIGHT AND EVALUATION

TOGETHER WITH

ADDITIONAL VIEWS

OCTOBER 19, 1988.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
89-545 WASHINGTON : 1988

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

Established by H. Res. 658, 95th Congress, 1st Session

LOUIS STOKES, Ohio, *Chairman*

ANTHONY C. BEILENSON, California
ROBERT W. KASTENMEIER, Wisconsin
ROBERT A. ROE, New Jersey
MATTHEW F. McHUGH, New York
BERNARD J. DWYER, New Jersey
CHARLES WILSON, Texas
BARBARA B. KENNELLY, Connecticut
DAN GLICKMAN, Kansas
NICHOLAS MAVROULES, Massachusetts
BILL RICHARDSON, New Mexico

HENRY H. HYDE, Illinois
DICK CHENEY, Wyoming
BOB LIVINGSTON, Louisiana
BOB McEWEN, Ohio
DAN LUNGREN, California
BUD SHUSTER, Pennsylvania

THOMAS K. LATIMER, *Staff Director*
MICHAEL J. O'NEIL, *Chief Counsel*
THOMAS R. SMEETON, *Associate Counsel*
BERNARD R. TOON II, *Professional Staff Member*

SUBCOMMITTEE ON OVERSIGHT AND EVALUATION

ANTHONY C. BEILENSON, California, *Chairman*

DAN GLICKMAN, Kansas
MATTHEW F. McHUGH, New York
BERNARD J. DWYER, New Jersey
CHARLES WILSON, Texas
BARBARA B. KENNELLY, Connecticut

BOB McEWEN, Ohio
BUD SHUSTER, Pennsylvania
HENRY J. HYDE, Illinois

RICHARD H. GIZA, *Professional Staff Member*
DIANE S. DORNAN, *Professional Staff Member*

House of Representatives,
Permanent Select Committee on Intelligence,
Washington, DC, October 19, 1988.

Hon. Jim Wright,
The Speaker, House of Representatives,
Washington, DC.

Dear Mr. Speaker: I submit the enclosed report on "U.S. Counterintelligence and Security Concerns: A Status Reoprt, Personnel and Information Security" prepared by the Subcommittee on Oversight and Evaluation of the Permanent Select Committee on Intelligence and approved by the Committee for printing under the Rules of the House.

Sincerly,

Louis Stokes,
Chairman.

CONTENTS

LIST OF WITNESSES

WEDNESDAY, MAY 18, 1988

Mr. John F. Donnelly, Assistant Deputy Under Secretary of Defense (Counterintelligence and Security), Department of Defense.

Mr. Thomas J. O'Brien, Director, Defense Investigative Service, Department of Defense.

Dr. Carson Eoyang, Director, Defense Personnel Security Research and Education Center, Department of Defense.

Dr. Eli Flyer, Manpower Program Analyst, Monterey, CA (submitted written statement for the record).

WEDNESDAY, JUNE 15, 1988

Mr. Henry P. Mahoney, Associate Deputy Director for Administration, Central Intelligence Agency.

Mr. Gardner Hathaway, Associate Deputy Director for Operations for Counterintelligence, Central Intelligence Agency.

Mr. Philip T. Pease, Director of Security, National Security Agency.

Calendar No. 640

100TH CONGRESS *2d Session*	HOUSE OF REPRESENTATIVES	REPORT 100–1094

U.S. COUNTERINTELLIGENCE AND SECURITY CONCERNS: A STATUS REPORT PERSONNEL AND INFORMATION SECURITY

OCTOBER 19, 1988.—Committee to the Committee of the Whole House on the State of the Union and ordered to be printed.

Mr. STOKES, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

I. INTRODUCTION

The Oversight and Evaluation Subcommittee of the House Permanent Select Committee on Intelligence recently completed hearings held in executive session to assess intelligence and defense community progress in addressing the findings and recommendations contained in the Committee's report entitled *"U.S. Counterintelligence and Security Concerns—1986."* That report highlighted numerous security problems throughout the defense and intelligence agencies of the U.S. Government which were discovered during the Committee's examination of several damaging and highly publicized espionage cases which occurred over the last several years.

The security problems identified included:

—Weaknesses in the process of selecting personnel for initial employment;

—An inattention to the security consciousness of current employees;

—A lack of appreciation for the security risks posed by former employees who had previous access to sensitive secrets; and

—The fact that financial gain, not ideology, is the primary motivation among most spies apprehended in the United States in recent years.

The Committee also found that:

—Too many security clearances are granted by the government; and

—Too much information is classified.

In this first of a series of inquiries into remedial steps being taken by the executive branch, the Subcommittee focused on personnel and information security. Personnel security is particularly important since virtually all of the most damaging espionage losses in recent years have been the result of the actions of an individual and not a result of a physical or technical penetration of a sensitive facility by a hostile foreign intelligence service. For example, the personnel security screening process failed dramatically in the cases of Edward Lee Howard, Jonathan Pollard, and Glen Michael Souther. The recent Souther case is particularly distressing, since the security background investigation conducted on him failed to turn up the fact that he was actively engaged in espionage at the time. Eighteen months after he was granted access to sensitive compartmented information, he defected to the Soviet Union.

The Subcommittee received testimony for the record from defense agency and intelligence community witnesses. In addition, a former Defense Department official who served in numerous personnel security-related positions provided a written evaluation of the Department's personnel security programs. Through this inquiry, the Subcommittee found that numerous efforts are under way in the executive branch to address problems identified in various congressional reports and executive branch study panels over the past few years. While some positive steps have been taken, progress has been limited to improvements within the context of the government's existing programs.

The evaluation of an individual's ability to protect sensitive national security information currently focuses on two distinct periods—a pre-employment investigation phase, followed by routine security evaluations while that person is employed. The record of previous espionage cases and testimony from government witnesses indicated that a third area may be of equal importance—that of the former employee who once had access to classified information and is now out of the direct control of the government's personnel security system. While the executive branch has attempted to improve its programs in the first two areas, the third has been addressed only in a limited way.

This report addresses each of these areas and makes the following findings.

II. Findings

GENERAL

● The Subcommittee found that both the Department of Defense and the intelligence community have initiated steps to improve the scope and quality of personnel security programs. Many of these efforts, however, have suffered from a lack of attention at the working level and the lack of a dedicated commitment of management to provide the necessary leadership and resources.

● The 1985 "year of the spy" spurred some initial improvements in the poor state of U.S. counterintelligence, although witnesses acknowledged there is still a long way to go. Moreover, at least in the area of personnel security, the 1986–87 burst of energy and support has largely dissipated. Momentum is being lost as numerous initiatives are stalled or slowed and as plans progressively are trimmed back.

● Attempted improvements thus far have focused on making the existing system work better at the margins and on incremental steps rather than on innovation and fresh thinking. Testimony indicates the need to step back and consider whether the underlying philosophy, focus and methods of this system are adequate. The usefulness and relevance of current security screening methods and security evaluation procedures require thorough reexamination.

● Personnel and information security continue to receive less attention than other security disciplines. While programs related to electronic countermeasures, surveillance, and physical security receive high levels of funding in the intelligence and defense communities, personnel and information security programs continue to go begging. This is especially bothersome inasmuch as virtually all known espionage losses in the United States in recent years have been a result of human weaknesses and not as a result of technical or physical penetrations of sensitive facilities.

● The large numbers of personnel security clearances and volume of classified information noted in the Committee's report of last year continues. While the Department of Defense has made progress in reducing clearances, this accomplishment appears to have been partially cosmetic and has been undermined by an upward trend this year. Effective oversight within the Department is nonexistent, and the accuracy of the clearance reductions reported is questionable. Continued management attention to this problem will be required to assure that any past achievements are not reversed.

● Security clearances can no longer be considered an infinite resource with no limit on their number. Management must carefully review and justify each request for a security clearance. Granting clearances based on the information requirements of the job, rather than tying them to individuals, would be a critical first step to enforcing this notion.

● Security oversight in Department of Defense Special Access Programs [SAPs] remains a problem. While policy guidance has been clarified, the military services, particularly the Air Force, continue to resist security inspections by an independent oversight entity.

● Turf consciousness and resistance to centralization long have plagued the U.S. counterintelligence community and continue to impede consideration and implementation of different methods of organization.

● Improvement in personnel security practices on Capitol Hill remains an important priority. At present, there is not a central repository of clearances so one can determine the level of access granted to individual staff. The Senate has begun to implement some changes, and the House should make improvements as well.

PRE-EMPLOYMENT SECURITY CONCERNS

● Many of the government's existing personnel and information security programs are outmoded and require revision. Continued emphasis on pre-employment background investigations appears misplaced, since it is extremely rare that clearances are denied on the basis of these investigations.

● Security clearance adjudication procedures and training are a significant problem area, particularly in the Department of Defense. In many instances, adjudication criteria and guidance are not being followed. The resulting low standards explain why 99 percent of applicants are granted initial or continued access. In effect, a clearance normally is granted unless there is serious recent drug abuse, alcoholism, a criminal record or psychiatric problems. More difficult issues of integrity and character are avoided. Despite this lack of selectivity, the adjudication process has also become a major bottleneck in DOD's personnel security system, and is in dire need of at least partial automation. Centralized adjudication in the military services, a key recommendation of the Stilwell Commission, has proceeded slowly.

● The government's current National Agency Check [NAC] is inadequate for granting access to secret information. Recommendations for an expansion of its scope by numerous panels over the years have been ignored. Although this would require only about $10 million yearly, resources for such an expansion have never been budgeted.

● The Director of Central Intelligence, in cooperation with the Department of Defense and Office of Personnel Management, should finally implement as recommended by numerous panels a "single scope" background investigation for access to top secret and sensitive compartmented information [SCI]. Such a step might drop the current requirement for a 15-year life history review and add a more productive interview with the subject, while reducing costs. Intelligence agencies may wish to retain the 15-year personal history investigation. Interviews with relatives, now avoided, could also make background investigations more effective.

SECURITY EVALUATION OF CURRENT EMPLOYEES

● Recent espionage cases have highlighted the importance of "continuing evaluation"—the process of assessing an employee's reliability and suitability for continued access to classified information after gaining employment. The quality of such programs varies widely among the defense and intelligence agencies, and they are not receiving the attention they deserve.

● Increased efforts are required especially in the area of assessing financial vulnerability among personnel holding security clearances. With recent espionage cases showing an increasing tendency toward espionage for the sake of greed or relieving financial distress, employees' financial health must receive increased scrutiny. The executive branch needs to be more skillful in utilizing the automated data bases at its disposal that go beyond mere credit reports, such as reports of casino transactions, currency transactions, and foreign bank and financial accounts.

● The Subcommittee found that strict adherence to the "need-to-know" principle still appears to be receiving little serious attention among defense and intelligence agencies. Fear of leaks and espionage has sometimes led to over-compartmentalization that impedes efficiency and lowers the quality of analysis and of staffing for policy options. In general, however, the prevailing culture is lax, allowing casual exchange of information and unnecessary access.

● Not enough is done to promote security awareness. Intelligence collectors still appear to lack a counterintelligence focus. The Pollard case demonstrated the great value of security awareness by fellow employees as a tipoff to possible espionage. Some recent espionage cases also raise the possibility that U.S. intelligence should have picked up clues that something was amiss and taken appropriate action. Unfortunately, the tendency has been to rely on defectors and largely serendipitous information rather than identifying and persistently investigating problem areas.

● The general prejudice with which offices of security are viewed by employees is an issue demanding attention in all agencies. Too often, such offices invite disdain because of inadequate personnel training, overattention to minor physical security problems at the expense of larger counterintelligence concerns, lack of friendly contact with employees and lack of positive help with employee problems that might lead to a motive for espionage. Employees must be provided non-threatening opportunities and incentives to report possible security concerns involving themselves or coworkers.

POST-EMPLOYMENT ISSUES

● Given the damage that can be caused by former employees, the personnel security system must begin to pay attention to those who leave government service under adverse circumstances. Many agencies have no existing program to address this important area. The CIA has expanded an already existing post employment follow-up program, and their approach deserves attention throughout the intelligence and defense communities.

III. Pre-Employment Security Concerns

THE NATIONAL AGENCY CHECK

The National Agency Check [NAC] is currently required for access to information classified at the confidential or secret level. The NAC is also the first step in background investigations that are conducted for higher level clearances. It involves a routine review of FBI fingerprint files and a review of holdings at other agencies which might indicate previous employment, immigration status, foreign travel, or the prior holding of a security clearance with another federal agency.

Defense Department witnesses suggested that a more sophisticated National Agency Check is needed. The Director of the Defense Investigative Service [DIS] pointed out serious problems in using the current NAC as the basic investigative requirement for a secret clearance. He noted,

> The National Agency Check is not sufficient in my opinion for a secret clearance. While a NAC costs about $10, we . . . spend thousands for physical security measures in some programs (to protect) secret material, but for the people part of it, we are only willing to spend $10. All of our losses have come from people.

Recommendations by this Committee, the Stilwell Commission and other study panels for the addition of a credit check and written inquiry of former employers to be added to the NAC have not yet been implemented. It is inexcusable that the majority of people who require access to classified information are cleared at the secret level, and for these individuals, the government conducts only a NAC, seeking no financial or employment history information. The Committee finds this failure to act inexcusable. Testimony from professional security experts was unanimous that these two elementary criteria should have been made a part of the NAC years ago.

IMPROVING BACKGROUND INVESTIGATIONS

The background investigation is utilized in screening employees for access to information classified at the top secret level and for sensitive compartmented information. Two basic types of background investigation exist today—the basic Background Investigation [BI] and the Special Background Investigation [SBI]. The BI covers the last 5 years of the applicant's life or from his 18th birthday, whichever is shorter. It includes a NAC, inquiries of local law enforcement agencies, employment, and credit checks, and an interview with the subject being investigated. It does not include a neighborhood check but requires investigators to interview character references. The SBI covers the last 15 years of an applicant's life, including all points covered in a BI—except a subject interview. It also includes neighborhood investigations and a credit check. The scope of the SBI is determined by Director of Central Intelligence regulations, since it is required for clearances granting access to sensitive compartmented information [SCI] which involve intelligence sources and methods.

The Committee is concerned that the various pre-employment background investigations now in use are not effective in identifying security-related problems before employment. In testimony before the Subcommittee, a senior official of the Defense Department noted that,

> With regard to personnel security, we realize . . . that background investigations do not catch spies. That is not their purpose. Their purpose is to identify human vulnerabilities that can be exploited by hostile intelligence services.

The record of past espionage cases illustrates that the current investigations process fails dismally in this objective. It was disconcerting to hear the same official comment, "I do not see where there is a great deal to be gained by new approaches." The Subcommittee's conclusion is precisely the opposite given the fact that over 54 DOD personnel in the last 5 years have been identified and punished for espionage or serious security breaches, not including those involved in the recent Conrad case.

Concerning the screening of military personnel for sensitive positions, a former DOD official with 25 years' experience in personnel screening and security fields noted, "prescreening procedures . . . vary considerably in scope and quality . . . many people found suitable for highly sensitive positions . . . are later discharged for unsuitable behavior." He noted further,

> There is a compelling need to improve the quality of personnel assigned to highly sensitive positions. Considerable evidence has accumulated showing that many people are entered into these positions whose past behavior and conduct are unfavorable. Further, many individuals are retained in these positions after providing ample evidence of unreliability, unsuitability, and untrustworthiness.

Given the low turndown rates experienced in the Department of Defense, it is questionable whether the resources and time invested in doing background investigations on all personnel requiring clearances is warranted. Denial and revocation rates for the DOD on confidential, secret, and top secret clearances in fiscal years 1986 and 1987 were one percent. For sensitive compartmented information [SCI] clearances the revocation rate has actually dropped from 5.1 percent in fiscal year 1983 to 1.4 percent in fiscal year 1987. Given these rejection rates, the continued viability and cost effectiveness of the DOD's security background investigation process is seriously in question. Also, no DOD agency at present collects data indicating the reasons given for denial or revocation of clearances.

Because most of the intelligence agencies require a polygraph interview as a part of their security investigations, it is not possible to precisely determine the number of security disapprovals based solely on the background investigation. An example cited by CIA of contractor rejection rates indicated that for one sample the rejection rate based on a BI alone was 3 percent—another indication that the emphasis placed on the pre-employment BI deserves reexamination.

Concerning the actual information gathered in background investigations, intelligence community witnesses noted that positive information about an individual frequently is as valuable as derogatory information. At present, DIS reports contain largely derogatory information. This is a failing in current DIS reporting. It should be corrected, since the addition of positive information provides a good benchmark for later determining changes in an individual's attitudes and behavior.

Testimony also highlighted the need for investigations to contact a broader base of individuals who are not currently interviewed. Relatives, for example, have traditionally not been interviewed because of the presumed bias of any information they might provide. Relatives, however, often can be an excellent source of information. The Walker case demonstrated that relatives may have information of serious security concern which may not be available from other sources. The most recent example of this is the case of Naval reservist Glen Michael Souther, in which Souther's former wife was the first to raise allegations that he might be a spy. These allegations were initially ignored by Naval investigators, and unbelievably, Souther's former wife was not interviewed during the course of his special background investigation for access to sensitive compartmented information.

THE SUBJECT INTERVIEW

One investigative technique highlighted by witnesses was that of the subject interview. Testimony was unanimous that an initial interview with the subject of a security background investigation is one of the most useful tools for yielding information and is underutilized. One witness noted, "This very sensible approach to improving background investigations has still not yet received the attention it merits." Such an interview is currently a part of the background investigations done for top secret clearances but is not a part of the background investigation performed for access to sensitive compartmented information [SCI]. Witnesses indicated that it should be.

The Director of DIS noted, "It is our contention that the scope of coverage of the SBI has not kept pace with our changing society over the last 40 years. . . . The BI currently being used for top secret clearances was developed in 1980–81, while the SBI has not changed since World War II." BIs now conducted for access to top secret information include an in-depth subject interview. Numerous panels have recommended over the years that a universal background investigation encompassing one set of standards (time of coverage, interview requirements, etc.) be formulated for both top secret and SCI. This concept, known as a "single scope" background investigation, would provide more consistent standards for granting access to highly classified information. No action has been taken by the executive branch to implement a single scope background investigation. The Subcommittee believes this issue should receive high priority, and urges the Director of Central Intelligence to reinvigorate efforts to reach agreement among the relevant agencies for a single scope BI, incorporating a subject interview, for access to top secret and SCI information.

SECURITY CLEARANCE ADJUDICATION

Security clearance adjudication refers to the process whereby individuals analyzing data acquired in a personnel security investigation attempt to reconcile that data with standards for granting a clearance. If derogatory information is acquired during the conduct of an investigation, it is the adjudicator's responsibility to provide feedback to investigators to determine if this data can be reconciled or to make a recommendation not to clear the individual for access.

The Subcommittee found that while criteria for the granting of clearances are generally consistent with the protection of national secrets, their application across agencies vary widely. In many instances, the criteria and guidance are not being followed. Defense Department security professionals testified that the adjudication process has become the major bottleneck in the clearance process, and that the current methods used to accomplish the task are antiquated and in dire need of revision. Most personnel security investigation files currently are still maintained as paper dossiers and are processed through the mail or by courier systems which take considerable time and administrative effort.

The utilization of automated data processing technology and centralized clearance data bases is desperately needed. A Department of Defense research program is examining the development of an automated system that will provide early identification of cases which do not require prolonged adjudication review so that they can pass rapidly through the system. This could streamline the processing of "clean" cases while providing more time for anaylsis of problem cases and more effective use of limited resources.

Witnesses indicated that a shift in focus may be necessary whereby individuals are initially evaluated under the broad concept of employee suitability rather than from a strict security point of view. It was noted that this would ease the job of adjudicators, since it is more effective to deny an individual employment for suitability reasons rather than security reasons. This would cast off the negative stigma of being rejected as a "security risk" implied by the current system in denying a security clearance.

The training of adjudicative personnel throughout the government varies widely. While intelligence agencies have conducted formal courses of instruction for their adjudicative personnel for a number of years, the Department of Defense has just begun to offer formal training for its adjudicators. Previously, on-the-job training—often utilizing inexperienced personnel—has been the norm. One former DOD official stated, "The adjudication process in Defense is considered by many personnel security professionals to be seriously flawed. . . . Many adjudicators lack an appropriate background for making complex personnel assessments."

Until recently, numerous components of the military services and many of the defense agencies maintained their own adjudication offices. This often led to the inconsistent application of criteria for granting clearances, and a lack of control on the granting of security clearances. A consolidation of adjudication facilities among the military services has proceeded with limited success, with the Navy still not fully on line in consolidating its adjudication process. Numerous defense agencies continue to resist this concept, largely, it appears, for bureaucratic turf reasons. The concept of centralized adjudication, a key recommendation of the Stilwell Commission, has moved slowly in the DOD and will continue to do so unless high level management attention is directed at the problem.

IV. Security Evaluation of Current Employees

PERIODIC REINVESTIGATION

Recognizing the need to focus attention on the security consciousness of current employees, the defense and intelligence agencies have for some time conducted periodic reinvestigations [PRI] of those personnel holding top secret and SCI clearances. This reinvestigation involves a NAC, inquiries to local law enforcement agencies, a credit check, subject interview, and field interviews with coworkers and references.

These investigations are required every 5 years after initial employment, but the executive branch has had considerable difficulty maintaining this schedule. Recommendations by various panels to extend the coverage of PRIs to those holding secret clearances have not been implemented due to resource constraints. Testimony indicated that these investigations may have some deterrent effect on an employee contemplating espionage.

It is evident that the executive branch must learn to approach this problem in a more sophisticated way given the problems encountered in performing PRIs on schedule. If resources dictate only being able to do a portion of the PRIs due in any given year, the government should prioritize its resources to examine those who occupy the most sensitive of positions or who may be the most vulnerable to espionage.

Initial research conducted by the Defense Personnel Security Research and Education Center [PERSEREC] indicates that rigorous and timely reinvestigations of key personnel would identify more actual or potential cases of espionage than would pre-employment background investigations. Current PRIs could be improved by having them occur at random intervals based on the sensitivity of the position, rather than on the arbitrary 5-year schedule currently used.

Since the establishment of the Defense Investigative Service [DIS] in 1972, its staff has grown only slightly, while increases in the DIS workload have been dramatic. Backlogs of PRIs are endemic throughout the defense and intelligence agencies. Additional resources have been provided in previous years to DIS, CIA, and the National Security Agency for the purpose of reducing these backlogs, but they are not expected to be eliminated until 1990. For example, at the end of May 1988, the Defense Department had a backlog of 101,000 periodic reinvestigations. The estimated resources necessary to alleviate this deficiency and also conduct periodic reinvestigations on those employees holding secret clearances would have required an additional 1,300 positions and $50 million. The availability of such resources is highly unlikely given current resource constraints.

Officials from the Defense Manpower Data Center [DMDC], a central repository of personnel records on DOD employees, have offered numerous proposals in which automated data bases not currently used could assist personnel security professionals in "targetting" currently cleared personnel for periodic reinvestigations. Funds should be made available for selective testing to determine if such a concept is feasible.

CONTINUING EVALUATION

Continuing evaluation programs assess an employee on a daily basis and not just at the time of the PRI or during annual job performance reviews. They require a sensitive and enlightened management, cooperative employees and an office of security that is viewed as a positive force in the workplace—not the negative connotation in which it is normally viewed.

The Defense Department currently operates such a program for personnel involved in the handling of nuclear weapons. This program, known as the Personnel Reliability Program [PRP], offers a structured approach to evaluating an individual's performance on the job and brings together information from supervisors, coworkers and other sources relating to the individual's behavior and performance. Personnel who do not meet PRP standards are subject to temporary or permanent decertification from the program. While the PRP is primarily a personnel program, its prescreening, continuing evaluation and certification procedures largely parallel those standards used for security clearance eligibility.

When properly followed, programs such as the PRP might be extended to other highly sensitive positions and would provide valuable information to supervisors who must justify an individual's continued access to classified information. Other federal agencies are currently examining similar programs for personnel in sensitive positions. Such programs offer valuable opportunities for assessing security in the workplace, and their application deserves a thorough examination by all agencies. They offer a more comprehensive assessment of an individual's reliability than that currently offered by the arbitrary 5-year PRI.

To be effective, such programs will require a fundamental change in most offices of security and the provision of sufficient resources for investigation and training—areas where the Defense and intelligence agencies have been deficient.

Very little money and effort has been expended on security awareness. More attention should be paid to this area, since recent espionage cases demonstrate that frequently it is difficult to ascertain the possibility of espionage based upon lifestyle alone, even when background investigations and reinvestigations are conducted properly. The Pollard case demonstrated the value of a complementary approach, that of encouraging security awareness by fellow employees, who can report patterns of work activity potentially associated with espionage.

A number of recent espionage cases also raise the possibility that U.S. intelligence agencies should have picked up clues that sensitive information had been compromised and investigated them. The tendency to wait for defector or other corroborating information rather than carefully analyzing more ambiguous indicators and narrowing them down to specific programs or individuals, is unfortunate.

OFFICES OF SECURITY

A critical area requiring attention is that of how offices of security are viewed by employees. In many agencies, security personnel are viewed as "cops" who carry out a sanctions-oriented process in which the investigation of a security-related incident is viewed as a career damaging event that will follow one throughout his or her career.

The Committee is convinced that to effectively attack the problem of espionage, a system that requires incentives as well as sanctions is required. A senior DOD personnel security research official noted:

> Among the cleared population, especially among that group cleared for the most sensitive information, we should encourage management and command sensitivity to their people, both on and off the job. There should be more support, less coercion. There should be an opportunity to share problems at early stages with a supervisor or counselor who might be able to help, before the problem becomes desperate, unshareable, and a motive for illegal behavior like espionage (develops).

The professionalism of individuals working in personnel security was also highlighted as an area of concern. This report has already noted the lack of training provided to adjudicators. In the military services, a career in security is generally not regarded as a path to senior rank. A more effective program in both the defense and intelligence agencies is required to provide clear and attractive career tracks in personnel and information security. The National Security Agency has an excellent program in this regard, and we commend it to the attention of other agencies.

RESOURCE SHORTAGES

Testimony before the Subcommittee indicated that personnel and information security continue to receive less emphasis than other counterintelligence disciplines. In agencies as large as the Department of Defense, oversight is key to the effectiveness of any program. With a population of over 2.8 million cleared personnel, 1.1 million contractor personnel, and over 12,000 cleared contractor facilities, the Office of the Secretary of Defense has only six professionals overseeing the personnel and industrial security programs of the Department. This is a penny-wise and pound-foolish approach considering these personnel have access to the Nation's most sensitive data, especially those involved in designing, procuring and building our future weapons systems.

The Subcommittee has a keen appreciation for the importance of physical security and other counterintelligence disciplines to DOD and intelligence installations and facilities worldwide. Technical security remains especially important at our overseas missions, as evidenced by the problems at the new Moscow Embassy construction project and the discovery several years ago of bugged typewriters in the old Moscow Embassy complex. Emphasis on these disciplines alone, however, fails to recognize that a large majority of recent intelligence losses have resulted from the actions of a cleared individual who decided to betray his country, and not from hostile intelligence officers penetrating a secure facility.

While recent espionage cases point to obvious deficiencies in the DOD's personnel security program, witnesses confirmed that "personel security programs are not being given a higher priority in the DOD budget process." One indicator of this fact is the roller coaster fashion in which the Defense Investigative Service has been funded. After obtaining increased resources over the last several years, DIS experienced in 1988 a $9 million budget cut and a 13.1 percent cut in personnel. This action has resulted in the discontinuance of training, and the loss of experienced personnel to early-out retirement.

While a portion of this cut was due to reductions mandated in the defense agencies by the Goldwater-Nichols Military Reform Act, these decreases went well beyond those congressionally mandated reductions. As the Director of DIS noted before the Subcommittee, "Rather than moving forward, we are currently undergoing a significant retrenchment." This trend occurs in the face of a new draft executive order on personnel security awaiting action at the National Security Council which would require increased efforts by DIS and other agencies in the scope and frequency of their background investigations. Separating out physical and personnel security as separate budget line items would heighten the visibility of these programs and help prevent cuts.

PROLIFERATION OF CLEARED PERSONNEL

A primary concern of the Committee in its report of last year was the proliferation of cleared personnel throughout the government. The Department of Defense has noted that it has reduced its clearances department-wide from 4.2 million in 1985 to 2.8 million today. Clearances in industry were reduced from a level of 1.4 million in 1985 to 1.1 million today, and classified contractor facilities were reduced from 14,000 to 12,000.

While the Subcommittee was initially impressed with these reductions, further investigation indicated serious problems with both the accountability in these figures and their continued effect on the security environment. No data were collected on the specific categories of personnel (civilian, contractor or military) who lost their clearances and what the specific reductions were. DOD clearance data bases remain highly fragmented, and the Department does not plan to have all of its clearances cataloged in its central data base—the Defense Central Index of Investigations—until the year 1990.

The most recent figures available from the DOD indicate that clearances in some agencies are again experiencing an upward trend. When asked whether any formal audit was conducted to validate the numbers reported by the military services and defense agencies in the clearance reduction program, DOD witnesses repeated, "no formal action was taken . . . to validate the reductions." Due to a lack of resources in the Office of the Secretary of Defense, the DOD is totally dependent on the military services and defense agencies to monitor their own clearance reductions. Effective oversight is nonexistent, and the accuracy and currency of data bases on individuals holding clearances is poor.

Testimony from the intelligence agencies indicated that no real efforts are underway to reduce clearances among their staff employees. If anything, these numbers can be expected to grow. This problem is endemic in the intelligence community since nearly all staff positions require a security clearance. As one CIA official noted, "The growth in security clearances is primarily driven by program start-ups and increases in personnel ceiling. Hence, increases in the number of cleared personnel is in many ways beyond (our) direct control. . . ." CIA has reported progress in reducing the number of contractor clearances, however, with 6,000 fewer contractor personnel cleared today than in 1986.

NEED-TO-KNOW

Closely related to the numbers of clearances is the issue of "need-to-know." DOD witnesses were quite candid in their assessment that, "unfortunately, many DOD agencies have given this most vital precept casual attention in the past." Intelligence agency witnesses highlighted the inherent conflict between the need to share information among intelligence analysts in the performance of their duties while still adhering to strict need-to-know principles. While various layers of compartmentation are intended to enforce this doctrine, its observance in the workplace becomes more problematic. Officials noted that in the final analysis, need-to-know was largely a matter of personal discipline. While this is certainly a factor, it is the responsibility of management to assure that it is practiced routinely in the workplace. A continued expansion of current intelligence community programs in this area is essential, as the steps taken thus far appear to be largely cosmetic.

Fear of leaks and espionage has raised the danger of over-compartmentalization, whereby information is denied to working-level people who should have it. The need for analytical efficiency and thoroughly staffed policy options should be balanced against security concerns. However, the practice of assuming that possession of a certain clearance level allows access to all information at or below that level, and the tendency toward casual exchange of information with other cleared personnel is not justified. Such information often is sought as a mark of power and "insider" status, while the withholding of it is resented. Over-reliance on the polygraph as a foolproof indicator of loyalty also has helped perpetuate this culture.

The primary vehicle for accomplishing improvements in this area recommended by the Stilwell Commission was the implementation of a "billet" control system for top secret clearances. A billet system consists of tying personnel security clearances to a position rather than to an individual. In such a system, employees move into a specific job and are granted the level of security clearance required to perform their duties while in that position. Once they transfer or move on to another job, their access to classified information changes based on the security requirements of that job. Their access may be increased or decreased depending on the "need-to-know" requirements of the job.

In the Department of Defense, only the Air Force has implemented a system to control access by position. Both the Navy and the Army are far behind in implementing such a system, with no action on the horizon. No specific indications could be elicited from the DOD on how it is translating its tougher bureaucratese and regulatory language on need-to-know requirements into meaningful improvements in the workplace. The Subcommittee views this as a serious deficiency in the Department's ability to manage and control access to national security information, and reiterates its support for the recommendation of the Stilwell Commission that a billet control system be adopted DOD-wide for access to information classified at the top secret level and for sensitive compartmented information.

V. Post-Employment Security Issues

A relatively recent phenomenon is that of individuals committing espionage after their employment in the intelligence community. The Howard, Pelton, and Walker cases illustrate the severe damage that can be caused by former government employees. The legal, practical and ethical problems of reducing security risks among this population are formidable. First, the government's right to investigate or monitor former employees without clear and probable cause is subject to serious question. Investigating such individuals would be bound to raise both legal and political challenges.

Secondly, the potential pool of personnel to be monitored is large. In 1987 alone, over 300,000 individuals were separated from the military, most honorably discharged, many not. Among enlistees receiving background investigations in fiscal years 1980–84, 27,000 were separated for various reasons of unsuitability. Cleared employees leaving the defense industry each year may be on the order of tens of thousands. Formal terminations for cause among this civilian population probably understates the number of individuals who leave with negative or hostile attitudes toward either their employers or the government. To identify and track this large number of personnel would be exceedingly difficult and prohibitively expensive.

These difficulties notwithstanding, some protections must be pursued given the severe damage which can be inflicted by a former employee with highly sensitive program knowledge. Comprehensive exit interviews, voluntary outplacement services, and continuing communication with separated employees are all steps that are being examined or taken in the intelligence community. Ideally, post employment follow-ups should be an integral part of any continuing evaluation program. In the DOD community, monitoring the tens of thousands of DOD personnel leaving sensitive positions could be a staggering task unless some form of automated prescreening of cases is conducted. It is significant that the DOD does not now keep track of the number of DOD employees who hold clearances and are released or reassigned for security reasons. This should be remedied, as these may be some of the very personnel who might commit espionage if they harbor hostile feelings toward the government.

RESPONSE TO THE HOWARD CASE

The Edward Lee Howard defection was one of the most serious losses in the history of U.S. intelligence. As one CIA official described it to the Subcommittee,

> . . . the things Howard gave to the Soviets were . . . unquestionably some of the most important operations we have ever run in the Soviet Union . . . what he did to us was devastating. . . . There is no question (when) you look at the record, it will show you that the agency did not do its job properly. . . .

This candid assessment indicates both the seriousness with which the agency took this case and the failures present at the time in its personnel security system. After a period of serious introspection and an Inspector General investigation, the CIA has taken numerous steps to address the problems encountered in the Howard case. This involved addressing both organizational problems and the level of resources dedicated to counterintelligence.

Through the creation of a new Counterintelligence Center, the agency has attempted to consolidate numerous functions in a central office whose director reports•to the DCI. The head of this office is theoretically responsible for the entire counterintelligence program in CIA, to include budgeting, planning, research and analysis, operations, and the detection of penetrations by hostile intelligence services worldwide, as well as enhancing coordination with other CIA offices and the FBI.

In addition to the creation of the Counterintelligence Center, several other steps to alleviate concerns flowing from the Howard case were highlighted in testimony to the Subcommittee:

—Counterintelligence staff are now included on all personnel decisions in which an employee is being separated from the agency under adverse circumstances. A counterintelligence risk assessment is required before any decision is made on terminating an employee.

—Steps have been taken to ensure that employees being separated for security reasons are fully aware of their appeal rights.

—The staff responsible for following up with former employees dismissed from the agency has been augmented, and financial and career counseling programs for personnel leaving the agency and former employees have been expanded.

—A memorandum of understanding has been signed between the CIA and FBI to govern the future handling of cases with possible counterintelligence implications. This formalizes what before was an ad hoc process—one which broke down during the Howard case with disastrous results.

—The assignment process for new agents to sensitive posts has been revised, with a special panel now screening and approving all new candidates. Interpersonal contact between new officers and management has been expanded.

—All relevant offices within CIA now sit on the various review panels for trial period employee security evaluations and adverse personnel actions.

In receiving testimony on these remedial steps, the Subcommittee was reasonably assured that the CIA has made an effort to address the problems exhibited in the Howard case. Many of these problems had as much to do with organizational culture as they did with resources. One agency official remarked, "We had a counterintelligence approach within the DO (the Directorate of Operations) . . . that was totally divorced from the culture in (the office of) security." While many of these steps should have been taken years ago, the Subcommittee supports their initiation and hopes that agency counterintelligence and security managers will remain vigilant to the concerns they address.

VI. Information Security

The Subcommittee was not impressed with testimony provided on controlling the growth in classified information. Regarding Defense Department programs, a senior Defense official noted, "I am not so certain that the amount of original classified information is excessive. I think that the real problem is that we do not get time to go back and review that which could be unclassified after, say, 5 years if we had time." He later noted, however, "With our efforts to maintain control over our technical as well as our classified information, we have our hands full handling the tremendous volumes that we face."

While DOD security regulations have required since 1986 that offices not retain classified documents deemed not permanently valuable over 5 years, and have required a yearly cleanout day, the implementation of these programs appears poor at best. DOD witnesses were frank in their statements that progress was not being made in these areas.

The Subcommittee found efforts in the intelligence agencies to be similarly weak. While the CIA noted a reduction in its original classification decisions last year, the progress was unimpressive. Their efforts to declassify data have centered largely around World War II era documents relating to the Office of Strategic Services.

One area of particular interest to the Subcommittee was the disclosures made last year in the publication of the book *VEIL* by *Washington Post* reporter Bob Woodward. At the urging of the Committee, the CIA conducted an investigation to ascertain the origins of the disclosures. During questioning from members of the Subcommittee, agency officials remarked, "While no hard evidence has surfaced pointing to a particular suspect, reasoned speculation indicates certain current and former agency employees may have been the purveyors of classified information to Woodward." Another agency official stated, ". . . I don't think there is a question . . . I think it came from within the agency. There is no question about that."

The agency has finally brought its investigation to a conclusion. Agency officials initially told the Subcommittee that these leaks were of utmost concern, and they admitted their frustration that, "To date, we have not devised a way to deal promptly and effectively with people who have violated the trust reposed in them."

VII. Special Access Programs

Related to the issue of controlling classified information in the aggregate is the oversight of Special Access Programs, known as SAPs. These controlled access programs are primarily utilized by the military services to protect procurement programs involving especially sensitive technologies. A recent DIS study of security oversight in SAPs notes that security is often lax and does not meet high standards. Deficiencies noted included inadequate security inspections, poorly qualified inspection personnel, an over-emphasis on physical security measures, and a deference to contractors in doing their own security inspections.

DOD has taken action to improve the security administration of SAPs, but some of these improvements have been cosmetic. Regulations have been rewritten, a security manual published, and SAPs must now be approved by the Secretaries of the military departments or the Deputy Under Secretary of Defense for Policy. Implementation, however, has been less than effective. DIS testimony noted, "In practice, the necessary improvements in the implementation of policy have still not been made at the level where the information is most vulnerable—when entrusted to the contractor."

It was also brought to the attention of the Subcommittee that a new phenomenon known as "gray programs" is also causing considerable confusion. These programs are so called because they occupy the gray area between normal security procedures and authorized special access programs. They employ unofficial names such as "Special Need to Know." Such programs currently have no basis in DOD regulation but resemble SAPs. Many are exempted from DIS security inspection responsibility, as are some SAPs. DOD witnesses indicated the Department's determination to do away with these programs, and the Subcommittee endorses continued vigilance in this area.

Senior DOD management has addressed the problem of SAP security oversight, but the military services, principally the Air Force, continue to resist independent security evaluation by anyone other than the service itself or the contractor. Having the contractor perform the oversight over his program while excluding independent agencies like the Defense Investigative Service, all in the name of security, is a prescription for disaster. The Secretary of Defense should take immediate action to halt this practice.

VIII. Research: The Need for New Approaches

Meeting the challenges posed by a growing population of cleared personnel, both active and former employees, will require that the government develop new approaches to personnel security. This will require extensive research, as well as renewed attention by management. The creation of the Defense Personnel Security Research and Education Center [PERSEREC] by the Department of Defense is a highly positive step. Prior to the creation of this center, no agency of the Federal Government performed research which challenged the conventional wisdom of existing personnel security systems. The Subcommittee views this research as critically important and commends DOD for implementing the recommendation of the Stilwell Commission for increased research in this area. While this is a DOD research agency, its work has relevance for personnel security programs throughout the intelligence community.

DOD and the intelligence community should be supportive of PERSEREC's work, and provide the resources necessary for research to proceed. However, PERSEREC's research must be closely monitored so that proposed changes or modifications will have practical utility. To benefit from this research, the executive branch must be attentive and receptive to implementing proposed changes—even when those changes challenge the viability of the current system. The Committee stands ready to be supportive of senior intelligence and defense agency managers in this regard.

IX. Conclusion

Today's spy becomes involved in espionage as a result of both personal and situational factors, and most importantly, access to classified data. Most are amateurs, and few, if any, enter the military or civilian employment with the intent to commit espionage. Neither do they necessarily behave at the time of entry in ways considered unsuitable. These individuals are not identified as potential spies based on initial background information. Varying environmental circumstances—financial problems, job disappointments or poor choices in emotional involvements—later interact with individual character weaknesses to create the motivation necessary to initiate a relationship with a foreign intelligence service. These variables cannot be predicted accurately at the time of the initial background investigation. Sometimes they cannot even be detected during on-the-job security reviews. Whatever the exact usefulness of the security background investigations, these facts point out the importance of continuing evaluation of cleared employees as a critical component of the personnel security process. As one DOD research expert noted, ". . . continuing assessment is an area where (we) can potentially make major improvements if innovative procedures can be developed."

The improvements suggested in this report should in no way be construed as advocating a "big brother" approach. What they do commend is utilizing current state-of-the-art automated technologies coupled with a hands-on approach down at the lowest management level to better protect our nation's secrets. Bureaucratic policy revisions and the issuance of agency directives are simply not enough if they are not effectively implemented.

Since the Committee's report was released in January 1987, there have been several additional spy cases with the Navy's Glen Michael Souther and the Army's Clyde Lee Conrad being the most significant. In both, the background investigation and reinvestigation process failed dismally. It is well proven that hostile intelligence services are actively attempting to procure sensitive intelligence information and sophisticated military technologies. The government must do a better job in assuring that our cleared population will keep the highly important trust placed in them.

The attention of senior management must become more focused and sensitized to the importance of personnel and information security programs. Despite verbal acknowledgment that some espionage losses have been truly devastating and have negated enormous defense investments, top managers remain unwilling to budget relatively modest sums for improved counterintelligence and security measures that would help protect much larger investments. The U.S. Government as a whole still is not comprehensively addressing past counterintelligence and security problems, although consciousness has been heightened in some quarters. No substantive improvements can be accomplished if the most senior officials continue to ignore the warning signals that something is fundamentally wrong. In most cases, this does not require a large investment in resources. As CIA Deputy Director Robert Gates has noted, "When it comes to human counterintelligence, my view is it is primarily a management and people problem, and not a dollar problem."

The true catalyst for change rests with those senior officials who have the power to give these programs higher visibility and the will to aggressively pursue needed changes. Only then, along with the support of the President and the Congress, will the government be able to meet the human counterintelligence challenges facing us in the 1990's and beyond.

ADDITIONAL VIEWS OF REPRESENTATIVES McEWEN, SHUSTER, HYDE, LIVINGSTON, AND LUNGREN

These hearings touched only lightly upon the subject of unauthorized disclosures of classified information. Such disclosures have become rampant and cause enormous damage to U.S. intelligence collection, intelligence liaison relationships and U.S. foreign policy interests. In 1987, for instance, scores of confirmed, first-time intelligence leaks pertaining to CIA work were identified.

Vigorous steps should be taken to reverse this permissive, widespread culture. The Congress should pass legislation establishing criminal penalties for intentional unauthorized disclosures of classified information. Nonetheless, this would have little effect if investigations remain as perfunctory as they are at present.

Intelligence agencies often have claimed that only other executive agencies and the Congress are guilty of unauthorized disclosures. During the course of these investigations, we became convinced that even the Central Intelligence Agency has displayed a profound lack of interest in policing its own demonstrated problems, especially when these may involve prominent officials.

In response to the Howard espionage case, the CIA has made some much-needed improvements in its procedures and organization. We would not wish to imply, however, that the long-overdue creation of a Counterintelligence Center is necessarily an adequate of final answer.

Protection of "turf" has been an impediment to optimization and centralization of the entire U.S. counterintelligence effort. We remain concerned, for instance, about whether CIA's Counterintelligence Center has been given adequate authority over regional offices and about whether its location within the Directorate of Operations accords it sufficient independence within CIA.

The Counterintelligence Center probably is the only existing institution which can help centralize counterintelligence operations that cross agency and departmental lines. It has made some progress in this area, in part due to currently dominant personalities and an increased awareness of the gravity of the threat. However, its formal charter in this respect is very weak.

All agree that some salutory steps have been taken since 1985, both in personnel and information security and in overall counterintelligence policy. But we are greatly concerned that this is just a start, and that even the steps taken thus far are subject to reversal unless there is aggressive support at the highest levels both within departments and in the White House itself. As one witness observed with regard to personnel security:

> Therefore, although many initiatives were undertaken in 1985 and much progress was made during 1986 and 1987, those initiatives have now, for the most part, stalled.

Rather than moving forward, we are currently undergoing a significant retrenchment.

The depth of past losses has been theoretically acknowledged, but has not penetrated to the extent that we are willing to take determined and consistent action. Investment in counterintelligence often is not seen as cost-effective. Major portions of the U.S. government still are not fundamentally serious about counterintelligence, although consciousness has been heightened in some quarters.

Bob McEwen,
Ranking Minority Member,
Subcommittee on Oversight and Evaluation.
Bud Shuster,
Member, Subcommittee on Oversight and Evaluation.
Henry J. Hyde,
Ranking Minority Member of Full Committee.
Member, Subcommittee on Oversight and Evaluation.
Bob Livingston.
Dan Lungren.

○